

Magic Quadrant for DevSecOps Platforms

15 June 2026 - ID G00841436 - 34 min read

By Keith Mann, Thomas Murphy, [and 1 more](#)

DevSecOps platforms provide software engineering teams with an integrated set of capabilities that improve the developer experience across the software development life cycle (SDLC) and enable teams to deliver software quickly. This research evaluates DevSecOps platform vendors to help software engineering leaders make buying decisions.

Market Definition/Description

Gartner defines DevSecOps platforms as those with fully integrated and orchestrated capabilities for continuous secure solution delivery using DevSecOps practices. They are built around the continuous integration/continuous delivery (CI/CD) pipeline, including planning, creation, artifact management, quality engineering, change management, compliance, environment management, deployment and monitoring, with security integrated throughout, plus collaboration, tool simplification and delivery metrics. They are delivered as cloud-hosted services, with some options for on-premises deployment.

DevSecOps platforms simplify the creation, maintenance and management of the components required for the secure delivery of various types of software. Platforms create common workflows, policies and data models; simplify user access; provide development and test environments; and provide a consistent user experience (UX) to reduce cognitive load and drive efficiency. They lead to improved visibility, auditability and traceability for the secure software delivery value stream. This end-to-end view encourages a systems-thinking mindset and accelerates feedback loops.

Organizations use DevSecOps platforms to reduce the friction and maintenance costs inherent in custom toolchains, decrease manual handoffs, and address the lack of consistent visibility throughout the software development life cycle (SDLC). This enables product teams to deliver faster customer value without compromising security or quality. The DevSecOps platform market reflects the consolidation of technologies across development, security, infrastructure and operations to streamline software delivery.

DevSecOps platforms support multiple use cases, including, but not limited to:

- Agile software delivery — Operationalize agile practices.
- Cloud-native application delivery — Build and deliver cloud-native applications across cloud-specific, hybrid and multicloud environments.
- GitOps — Support the operation of applications and infrastructure configurations using declarative constructs stored in Git in a closed-loop, automated system.
- MLOps — Provide support for the management of machine learning (ML) models including orchestrated delivery of versioned, secure LLM-based solutions, agents and MCP services.
- Platform engineering and Infrastructure platform engineering (via IAC) — Provide tools to support the platform engineering team's delivery of managed platforms, pipelines and practices to support consistent secure development and delivery.
- Regulated delivery — Provide support for compliance, auditing, remediation, traceability and governance.

Mandatory Features

- Continuous integration via native support for build automation and the orchestration of verification and validation functions such as test automation, security scans and compliance scans
- Continuous delivery and release orchestration via native support for:
 - Ungated continuous deployment
 - Release orchestration with gated approval mechanisms (e.g., to meet regulatory requirements) and policy management
- Delivery of web applications including, but not limited to, containerized applications

- Orchestration of security functions (which themselves need not be native), such as:
 - Threat modeling
 - Security requirements
 - Software supply chain security
 - Security testing (SAST, DAST, SCA)
 - Web application and API protection
 - Runtime application security

Optional Features

- Team and product management insights:
 - Agile planning, including product planning, managing features and defects, roadmapping, backlog management, Kanban, and Scrum
 - User feedback, analytics, centralizing insights from user research, usage data and strategic goals to understand value, feasibility and usability.
 - Feature management, including feature flag management and experimentation
 - Software engineering intelligence (SEI), including value stream analytics, flow metrics, DORA metrics, developer productivity metrics (SPACE framework support) and developer experience metrics (DevEx framework support)
- Development support:
 - Integrated development environments (IDEs)
 - Unit testing framework support
 - Code review facilitation
 - Package management
 - Static code analysis
 - Internal developer portal
- Artifact management:

- Source code repository
- Secure artifact repository
- Container registry
- Software bill of materials (SBOM) support
- Artifact integrity and provenance tracking
- Quality engineering:
 - Performance testing, chaos testing, fuzz testing and automated acceptance testing
 - Test case management
 - Test selection, execution and flaky test identification/remediation
 - Code coverage analysis
 - Test platform support and quality metrics
 - Test data management
 - Test suite optimization
- Environment provisioning and management:
 - Cloud platform environment provisioning and management
 - Infrastructure provisioning
 - Configuration management
 - Configuration drift detection
 - Infrastructure as code
- Application monitoring and observability:
 - Collection of production telemetry (e.g., logs, metrics, events, traces)
 - Automated incident response support
 - Customer feedback collection

- Team collaboration:
 - Visualization of development workflows
 - Knowledge base
 - Pairing
 - Communication via messaging/chat
- AI augmentation:
 - Agentic AI-assisted and AI-powered continuous integration and deployment
 - Process optimization
 - Agentic workflows such as planning, review, code fixes and incident remediation
 - Analysis of SEI and telemetry data

Magic Quadrant

Figure 1: Magic Quadrant for DevSecOps Platforms





Gartner

Vendor Strengths and Cautions

Atlassian

Atlassian is a Leader in this Magic Quadrant. It offers the Atlassian DevSecOps platform, which includes the Software, Teamwork, Product and Service Collections. Atlassian currently supports both SaaS and on-premises deployment. Atlassian's operations are geographically diversified, and its clients span all sizes and sectors. In 2025, Atlassian expanded agentic AI capabilities to support the entire product delivery life cycle, as well as AI administration and compliance. These capabilities are integrated into its platform and teamwork graph. It also incorporated DX (acquired in 2025) into the Software Collection.

Strengths

- **Market understanding:** Atlassian's vision for utilizing AI to improve efficiency and efficacy throughout all phases of the product delivery life cycle (not just coding) reflects its comprehensive understanding of the needs of DevSecOps platform customers.
- **Market responsiveness/record:** Atlassian's unified platform provides tooling and AI support to address the needs of the various roles involved in the DevSecOps life cycle.
- **Customer experience:** Atlassian has focused on its SaaS offering and provides strong SLAs, security and availability, as well as growing support for data residency and regulatory compliance.

Cautions

- **Product strategy:** Atlassian's DevSecOps platform cannot be purchased as a single SKU except by enterprise customers.
- **Sales strategy:** In 2025, Atlassian announced that Data Center products would be retired by 2029, except for Bitbucket and Align. New customers are no longer able to purchase new Data Center subscriptions or new Marketplace Data Center apps, leaving Atlassian as the only vendor in the Leaders quadrant without a viable option for customers that need an on-premises solution.
- **Product execution:** The Atlassian DevSecOps platform provides fewer native capabilities for ensuring the security of solutions compared with other Leaders in this Magic Quadrant.

Buildkite

Buildkite is a Niche Player in this Magic Quadrant. It offers the Buildkite DevOps platform, which includes Mobile Delivery Cloud, Package Registries, Pipelines and Test Engine. Buildkite can be deployed as SaaS or hybrid SaaS. Buildkite's operations are based primarily in Australia and North America, and its customers span all sizes and sectors, with a concentration in the technology sector. In 2025, Buildkite added AI capabilities with a Model Context Protocol (MCP) server for AI agents and agentic workflow capabilities in Pipelines, as well as Test Engine improvements to mitigate flaky tests.

Strengths

- **Product execution:** Buildkite's highly scalable build agent architecture makes it well-suited to large AI model development. Customers with larger or more complex software development organizations tend to benefit the most.
- **Marketing strategy:** Buildkite has an effective strategy for delivering its message to customers and prospects, emphasizing the speed, scalability and continuous integration (CI) capabilities the platform provides. Customers gain a good understanding of how Buildkite integrates into their internal DevSecOps strategy.
- **Market responsiveness:** Buildkite's focus on a narrow part of the DevSecOps process enables it to quickly address the needs of its customers.

Cautions

- **Geographic strategy:** Buildkite's product architecture requires that customers use its SaaS control plane, which is hosted only in the U.S. and EU. Customers should evaluate their data-residency requirements as this architecture may restrict the ability to use this platform.
- **Overall viability:** Buildkite's niche product, lack of profitability, new management and limited market visibility constrain growth opportunities. Prospective customers should remain vigilant regarding Buildkite's long-term viability.
- **Business model:** Buildkite has a less extensive third-party plug-in ecosystem compared with other vendors in this Magic Quadrant. Customers might find that the ability to customize or extend the product with supported plug-ins and extensions is limited.

CircleCI

CircleCI is a Niche Player in this Magic Quadrant. It offers CircleCI, which includes support for hosted and managed build infrastructure, self-hosted runners, test automation, insights into build performance and support for the CI/continuous delivery (CD) of large language model (LLM)-enabled apps. CircleCI can be deployed as SaaS or on-premises. CircleCI's operations are geographically diversified, and its customers span all sizes across many sectors, with the greatest concentration in the technology sector. In 2025, CircleCI added support for platform engineering teams with a platform team toolkit, an MCP server to enable conversational interaction with CI operations through AI

coding assistants, and early access to its Chunk Autonomous Agent and Smarter Testing capabilities.

Strengths

- **Market understanding:** CircleCI has a good understanding of the DevSecOps market and its position as a provider that delivers a high-performance CI/CD platform optimized for speed that integrates with best-of-breed tools and platforms.
- **Product strategy:** The vendor continues to make platform investments to help customers remove downstream constraints that slow delivery, such as testing, deployment and security.
- **Customer experience:** Customers frequently cite the ease of getting started, developer support and advanced documentation for complex tasks, in addition to its dynamic developer community.

Cautions

- **Sales execution/pricing:** While sustaining profitability in 2025, CircleCI has continued to see a shift toward smaller deal sizes, with seat counts concentrated in smaller user ranges. Customers need to ensure that CircleCI meets their criteria for a viable partner.
- **Geographic strategy:** As enterprises move to the cloud and SaaS implementations, CircleCI's cloud data centers continue to be limited to the U.S. Customers should verify CircleCI's compliance with their data residency requirements.
- **Innovation:** CircleCI has not created innovative product capabilities that differentiate it from its competitors.

CloudBees

CloudBees is a Niche Player in this Magic Quadrant. It offers CloudBees, which includes CloudBees Unify, CloudBees CI (self-managed) and CloudBees CD/RO Classic (self-managed). CloudBees can be deployed as SaaS or on-premises. CloudBees' operations are mainly in North America and EMEA, and its customers span all sizes across many sectors. In 2025, CloudBees consolidated its offering into one platform, CloudBees Unify, while also adding support for more version-control providers, expanding support for security scanning tools and enhancing release orchestration.

Strengths

- **Market understanding:** CloudBees has a large historical customer base that allows the vendor to understand the challenges of DevSecOps adoption in large, regulated enterprises.
- **Customer experience:** CloudBees has a range of postsales programs to help ensure its customers are successful.
- **Product strategy:** CloudBees' product strategy emphasizes maintaining compliance in a complex technological landscape, enabling software engineering leaders to effectively harness AI while mitigating associated risks.

Cautions

- **Overall viability:** Despite remaining profitable, CloudBees is experiencing shrinking customer lists and sales revenue. Customers should remain vigilant regarding CloudBees' long-term viability.
- **Sales execution/pricing:** CloudBees products are priced higher relative to the competition, and customers likely will incur additional costs to implement a complete DevSecOps platform because CloudBees does not offer a comprehensive solution.
- **Innovation:** CloudBees has not created innovative product capabilities that significantly differentiate it from its competitors. Customers may find that other vendors are first to market with new features.

GitLab

GitLab is a Leader in this Magic Quadrant. It offers GitLab, which includes capabilities for planning, source code management, CI, deployment automation, observability, application security testing, software supply chain security, compliance reporting, value stream analytics and incident management. GitLab can be deployed as multitenant SaaS, single-tenant SaaS (GitLab Dedicated) or on-premises. GitLab's operations are geographically diversified, and its clients span all sizes and sectors. In 2025, GitLab expanded its AI to incorporate multiagent workflows across the SDLC, strengthened its AI governance capabilities and enhanced its SLAs.

Strengths

- **Product execution:** GitLab has a broad product strategy and platform that natively provides most of the capabilities associated with DevSecOps platforms. Customers benefit from a comprehensive platform that reduces the need for third-party products and provides the flexibility to integrate with third-party tools and AI solutions.
- **Sales strategy:** GitLab's versatile platform architecture provides feature parity between SaaS and on-premises options, including AI.
- **Customer experience:** GitLab has strengthened its SLAs to meet or exceed those of its competitors.

Cautions

- **Sales execution:** Gitlab shows limited sales partner success in Asia/Pacific.
- **Product strategy:** The GitLab platform lacks support for parts of the enterprise involved in the DevSecOps life cycle outside of software engineering organizations.
- **Employee growth and retention:** Changes in culture, leadership, transparency and employee churn are negatively impacting GitLab employee sentiment.

Google

Google is a Niche Player in this Magic Quadrant. Google's DevSecOps platform offering consists of Cloud Build and Deploy, Artifact Registry, Gemini Code Assist, Gemini Cloud Assist, Security Command Center, Secret Manager, Google Cloud Observability and Gemini Enterprise. Google's platform is available as a multitenant SaaS or self-hosted solution. Google's operations are geographically diversified, and its clients span all sizes and sectors. In 2025, Google enhanced its AI MCP capabilities, incorporated MLOps into its integrated development environment (IDE) and added a knowledge graph to represent cloud operations data.

Strengths

- **Geographic strategy:** Google's extensive cloud infrastructure allows it to serve customers around the globe and meet their data residency needs.
- **Market understanding:** Google has a strong AI vision of the future for DevSecOps and provides software solutions and the computing resources to support large, complex, AI-driven workloads.

- **Business model:** Google has built strong platform and developer ecosystems. These ecosystems enhance its value to customers developing cloud-native solutions.

Cautions

- **Product strategy:** Google's offering is a collection of tools not specifically developed for DevSecOps that have been combined into an end-to-end platform, rather than created through an overarching product strategy. Prospective customers may find that this makes adoption more challenging.
- **Product execution:** Google's DevSecOps platform is still nascent. Much of the promised functionality depends on products that are not generally available.
- **Sales strategy:** Google is still working to elevate its value propositions for business leaders above and beyond the technology features. IT leaders may find it difficult to understand the value that Google provides to the greater organization.

Harness

Harness is a Leader in this Magic Quadrant. It offers the Harness platform, providing a comprehensive suite of capabilities including CI/CD, security testing, API security, feature management and experimentation, infrastructure-as-code management, internal developer portal, software engineering insights, artifact registry, database DevOps, cloud cost management, chaos engineering and AI site reliability engineering. Harness can be deployed as SaaS or on-premises. Harness' operations are in North America, Europe, Latin America and India, and its clients span all sizes and sectors. In 2025, Harness strengthened security capabilities by acquiring Traceable and Qwint AI. It also expanded AI support with the delivery of 13 system agents and the creation of an AI Agent Marketplace for custom agent deployment.

Strengths

- **Product execution:** Harness' market understanding and vision have yielded strong product features in areas such as agentic AI, security and MLOps.
- **Product strategy:** Harness' flexible delivery model enables customers to buy the entire platform or individual components. Harness has effectively extended and integrated open-source solutions along with acquisitions to create a unified DevSecOps platform.

- **Market responsiveness/record:** Harness spotted trends early and succeeded in building technical foundations that enable it to respond quickly to emerging market and customer demands, such as ML capabilities that have evolved into agentic AI capabilities today.

Cautions

- **Sales execution:** Harness' investment in its partner network has yet to result in more partner-led sales. Clients in some geographies looking to leverage Harness' partner network might find that these partners are still new to the platform and cannot yet provide service and support at the same level as more established partners.
- **Marketing execution:** Harness' marketing messages continue to fail to address the needs of senior management (C-suite), making them less likely to appeal to the leaders making purchasing decisions.
- **Customer experience:** Harness' SLAs provide availability and response times that are lower than those of its competitors.

HCLSoftware

HCLSoftware is a Visionary in this Magic Quadrant. Its DevSecOps platform consists of DevOps Loop (delivered only as a self-hosted, Kubernetes-native platform), HCL AppScan and HCLTech AI Force (both available as SaaS or self-hosted). HCLSoftware's customer base is mainly in the U.S., Europe and Asia, and its clients span all sizes and sectors. In 2025, HCLSoftware expanded the MCP-based automation within Loop and extended AppScan DAST to cover LLM-specific risks. It enhanced AppScan 360° to include on-premises software composition analysis (SCA) with software bill of materials (SBOM) support and integrated interactive application security testing (IAST) and improved reporting of metrics.

Strengths

- **Product strategy:** HCLSoftware has built a strong end-to-end platform that provides capabilities that are composable (and compatible) with existing customers' environments and toolsets.
- **Market responsiveness:** HCLSoftware's 2025 releases and roadmap for 2026 closely reflect customer feedback.

- **Geographic strategy:** The vendor offers data center support for SaaS in all regions except APAC and support for data-residency requirements.

Cautions

- **Sales execution/pricing:** The license cost for the platform, on a per-user basis, is one of the most expensive among vendors in this Magic Quadrant. HCLSoftware DevOps Loop is an all-in platform where a customer must purchase the top-tier license to get all features of the platform.
- **Sales strategy:** HCLSoftware DevOps Loop platform is available only as a self-hosted product. Customers can choose to host the platform in their own data center or in the cloud.
- **Product execution:** Much of the HCLSoftware DevOps Loop platform is built on existing DevSecOps solutions and practices. Customers using more modern approaches may find it difficult to adopt HCLSoftware DevOps Loop.

IBM

IBM is a Visionary in this Magic Quadrant. Its IBM DevOps Loop platform provides capabilities spanning planning to deployment and testing. Delivered only as a self-hosted Kubernetes platform, it shares the same core software offering as HCLSoftware's platform, except for its unique AI component. IBM's customer base is mainly in the U.S. and Europe, and its clients tend to be larger enterprises across all sectors. In 2025, IBM introduced agentic AI support, specialized AI assistants and full modeling capabilities with AI-augmented source code generation.

Strengths

- **Product strategy:** IBM DevOps Loop is a broad platform providing support for requirements, architecture and design, testing, security, AI and governance to support regulatory requirements.
- **Innovation:** IBM Research is one of the world's largest corporate research organizations, with thousands of researchers. Unique, deep innovations from IBM, such as support for quantum workload development, can be applied to the platform.
- **Geographic strategy:** IBM has strong global coverage that is enhanced by a large, geographically diverse partner network.

Cautions

- **Sales strategy:** IBM DevOps Loop is available only as a self-hosted product. Customers can choose to host the platform in their own data center or in the cloud.
- **Sales execution/pricing:** The license cost for the platform, on a per-user basis, is one of the most expensive of all the vendors in this Magic Quadrant. IBM DevOps Loop is an all-in platform where a customer must purchase the top-tier license to get all features of the platform.
- **Product execution:** Most of the IBM DevOps Loop platform (with the notable exception of IBM's AI solution) is built on existing DevSecOps solutions and practices. Customers using more modern approaches may find it difficult to adopt IBM DevOps Loop.

JetBrains

JetBrains is a Niche Player in this Magic Quadrant. Its JetBrains DevOps platform includes Qodana, TeamCity and YouTrack, which provide code quality, CI/CD and planning features, respectively. JetBrains' products can be deployed as SaaS or on-premises. JetBrains' operations are geographically diversified, and the vendor does not disclose the size or nature of its clients. In 2025, JetBrains added YAML alongside Kotlin DSL and a drag-and-drop visual editor for creating and maintaining pipelines in TeamCity. JetBrains also added MCP server and n8n integrations to connect YouTrack workflows with AI-powered tools.

Strengths

- **Overall viability:** While small, JetBrains has been profitable for the last 10 years and continues to grow.
- **Product execution:** JetBrains' focus on a small but important subset of DevSecOps capabilities has allowed it to produce tools that enhance developer productivity, such as strong IDEs.
- **Market responsiveness/record:** JetBrains continuously monitors changes in the market and customer needs when introducing new platform capabilities. Product roadmaps reflect user feedback and lessons learned from observing customer usage.

Cautions

- **Innovation:** Other than support for AI, JetBrains continues to show little innovation in its DevSecOps tools. Customers find that other vendors are first to market with new features.
- **Product strategy:** JetBrains continues to focus primarily on developer-centric capabilities, which makes the vendor's product strategy narrower than its competitors. Customers find that this does not address the needs of all DevSecOps users.
- **Geographic strategy:** JetBrains' SaaS offering supports only three regions. JetBrains supports data-residency requirements only for the EU.

Microsoft

Microsoft is a Leader in this Magic Quadrant. It offers two platforms, GitHub and Azure DevOps, which provide comprehensive capabilities, including CI/CD pipelines, advanced security, project planning and AI coding assistants. Both GitHub and Azure DevOps can be deployed as SaaS or on-premises. Microsoft's operations are geographically diversified, and it has clients of all sizes across all sectors. In 2025, Microsoft expanded its agentic DevSecOps capabilities with the Copilot Code Review Agent, extended existing AI governance and compliance controls, and enhanced GitHub Projects and Issues for AI-enabled workflows.

Strengths

- **Overall viability:** Microsoft has established a global presence in terms of research and development, sales and support, and cloud data center reach and capacity. Given its longevity, size, continued customer growth and integration of other DevSecOps solutions with Microsoft's offering, customers can be confident that Microsoft will sustain business continuity.
- **Business model:** Microsoft has built a strong ecosystem around its DevSecOps platform. Customers gain access to a wide range of native capabilities and third-party products and services via, for example, GitHub Marketplace, extensions and APIs.
- **Market understanding:** Microsoft's foundation in AI code agents, along with its large customer base, has given Microsoft an excellent understanding how AI will impact the future of DevSecOps.

Cautions

- **Market responsiveness:** GitHub's focus on AI has reduced its responsiveness to market demands for core DevSecOps functionality. Customers may find that other vendors are earlier to market with new core DevSecOps features.
- **Product strategy:** Microsoft's DevSecOps product strategy continues to include two products, Azure DevOps and GitHub. Clients must decide what mix of those two products suits them best.
- **Sales strategy:** Microsoft's pricing model is increasingly moving from per-seat to consumption-based pricing. This move makes its pricing model complex, increasing difficulty for customers to manage costs.

Octopus

Octopus is a Niche Player in this Magic Quadrant. It offers Octopus Deploy, which includes Codefresh and Codefresh GitOps Cloud. Octopus' products can be deployed as SaaS or on-premises. Octopus' operations are geographically diversified, and it has clients of all sizes across all sectors. In 2025, Octopus launched support for platform engineering teams with Platform Hub and added an MCP server, AI assistants and monitoring to help teams safely troubleshoot Argo CD.

Strengths

- **Overall viability:** Octopus continues to show success, allowing it to sustain its current strategy of focusing on CD product capabilities. Customer and employee surveys and financial results continue to show the ability for continued success.
- **Customer experience:** The vendor offers effective service and customer support, along with a multichannel community ecosystem to enable peer collaboration, feedback exchange and product input.
- **Market responsiveness/record:** Octopus is highly focused on enhancing CD product capabilities to support the priorities of its core customers.

Cautions

- **Market understanding:** Octopus' focus on continuous delivery limits the breadth of its vision. Customers must look elsewhere for other elements of their DevSecOps strategy.

- **Product strategy:** Despite purchasing Codefresh in 2024, Octopus has not incorporated Codefresh capabilities into its overall product strategy to support developers' needs.
- **Innovation:** Octopus has not innovated in areas of the DevSecOps life cycle other than CD. Customers may find that other vendors are first to market with new features.

OpenText

OpenText is a Niche Player in this Magic Quadrant. The OpenText DevSecOps platform consists of OpenText Core Software Delivery Platform (SaaS), OpenText Software Delivery Management (self-hosted), OpenText SDP DevOps (PulseUno), OpenText Project and Portfolio Management, OpenText Core Application Security (Fortify), OpenText Deployment Automation and OpenText Connect Synchronizer. OpenText products can be deployed as SaaS or on-premises. OpenText's operations are geographically diversified, and it has clients of all sizes across all sectors. In 2025, OpenText enhanced its platform with AI agents for functional and performance testing for test generation, execution and test result analysis.

Strengths

- **Product strategy:** OpenText's end-to-end platform supports the DevSecOps life cycle, with built-in governance and compliance, AI and software testing, and application security capabilities.
- **Market responsiveness:** OpenText continues to play to the historical strengths of its product suite, listening closely and responding to the needs of its customers. Its roadmap is driven more by customer needs than by the competition.
- **Customer experience:** OpenText provides global customer support with strong response times, SLAs and service-level objectives (SLOs).

Cautions

- **Innovation:** OpenText shows little innovation in its DevSecOps tools outside of testing. Customers find that other vendors are first to market with new features.
- **Sales execution:** OpenText's global partner network has not led to a significant customer base outside of North America and Europe.

- **Geographic strategy:** OpenText's SaaS offering supports only three regions. Customers needing to comply with data-residency requirements may have only the self-hosted option.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

- Google
- HCLSoftware
- IBM
- OpenText

Dropped

- Huawei

Inclusion and Exclusion Criteria

The following inclusion criteria represent the specific attributes a vendor must have to be evaluated in this Magic Quadrant.

Market Participation Inclusion Criteria

To qualify for inclusion, providers need to meet the following criteria as of 1 January 2026:

- Provide a dedicated, generally available (GA) DevSecOps platform. General availability means the product or service is available on a public-facing price sheet/card for

purchase directly by clients. Providers must be able to furnish the link to a pricing page for their DevSecOps platform.

- Sell the solution directly to paying customers without requiring them to engage in professional services. Providers must provide at least first-line support for these capabilities, including the use of bundled open-source software. This includes, but is not limited to, comprehensive product documentation, installation guidance (e.g., build runners, Kubernetes cluster setup) and reference examples (e.g., in the case of pipelines-as-code).
- Demonstrate an active product roadmap, go-to-market and selling strategy for the solution, including all standard capabilities as described in the market definition.
- Have phone, email and web customer support. Providers must offer a contract, console/portal, technical documentation and customer support in English (either as the product's default language or as an optional localization).
- Have at least 15% of their paying customers in two of the following three geographic regions:
 - U.S. and Canada
 - Europe (including the U.K. and Ireland)
 - Asia/Pacific

Platform Capabilities Inclusion Criteria

The DevSecOps platforms must offer native support for the following standard capabilities as described in the market definition:

- Continuous integration via native support for build automation and the orchestration of verification and validation functions such as test automation, security scans and compliance scans
- Continuous delivery and release orchestration via native support for:
 - Ungated continuous deployment
 - Release orchestration with gated approval mechanisms (e.g., to meet regulatory requirements) and policy management

- Delivery of web applications including, but not limited to, containerized applications
- Orchestration of security functions (which need not be native), such as:
 - Threat modeling
 - Security requirements
 - Software supply chain security
 - Security testing (SAST, DAST, SCA)
 - Web application and API protection
 - Runtime application security

Magic Quadrant Exclusion Criteria

Vendors are excluded from the analysis if:

- The primary use case for the DevSecOps platform is the delivery of mobile applications, low-code applications, packaged business applications or SaaS-based applications (i.e., developing, extending, configuring or customizing applications such as Salesforce, Dynamics 365, Oracle, SAP or ServiceNow). The market needs and expected platform capabilities for these use cases differ from the market definition of this Magic Quadrant.
- The platform is only sold as part of custom software development or professional services engagements (e.g., professional services providers using a custom solution for their clients).

Evaluation Criteria

Ability to Execute

We specifically looked for excellence in these areas:

Product or service: Product planning, software development, continuous integration, continuous delivery and release orchestration, configuration automation, monitoring,

observability and operations support, a managed version of open-source components in the platform, an integrated platform for orchestration, collaboration and visualization, software delivery metrics, secure delivery, and AI augmentation and accessibility

Overall viability: Revenue growth, employee growth and retention, and healthy financials, including funding status

Sales execution/pricing: Customer growth and sales momentum, partner strength, and customer wins and renewals

Market responsiveness/record: Business agility and customer responsiveness

Marketing execution: Articulation of value proposition to different audiences and thought leadership in marketing

Customer experience: Customer vote of confidence, customer satisfaction and commitment to improving customer experience

Operations: Quality and effectiveness of programs to support the platform and engage customers

Ability to Execute Evaluation Criteria

<i>Evaluation Criteria</i>	<i>Weighting</i>
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	High
Market Responsiveness/Record	High
Marketing Execution	Low
Customer Experience	High

<i>Evaluation Criteria</i>	<i>Weighting</i>
Operations	NotRated

Source: Gartner (June 2026)

Completeness of Vision

We specifically looked for excellence in these areas:

- Market understanding:** Strategic vision for the market, understanding of competitive landscape, and active product roadmap and path forward
- Marketing strategy:** Linking market understanding to messaging
- Sales strategy:** Adopting multiple sales motions, growing the business, and licensing and pricing models
- Offering (product) strategy:** Compelling product vision, competitive differentiation and moving from a DIY toolchain to a platform approach
- Business model:** Building a platform ecosystem and OEM-centric/partner-centric business model
- Vertical/industry strategy:** Specialization for industry verticals and domain expertise
- Innovation:** Innovation as a competitive advantage, organic innovation and inorganic innovation
- Geographic strategy:** Platform capabilities to support multiple geographies, demonstrate sales strategy across geographies and demonstrate partner strategy across geographies

Completeness of Vision Evaluation Criteria	
<i>Evaluation Criteria</i>	<i>Weighting</i>
Market Understanding	High
Marketing Strategy	Low

<i>Evaluation Criteria</i>	<i>Weighting</i>
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Low
Vertical/Industry Strategy	NotRated
Innovation	High
Geographic Strategy	Medium

Source: Gartner (June 2026)

Quadrant Descriptions

Leaders

Leaders have a deep understanding of the DevSecOps platform market and stand out in this highly competitive global market. They have a record of strong execution and can influence the market’s direction through thought leadership and resources. Leaders also have a clear vision and well-defined product roadmap.

The most distinctive attribute of Leaders in this market is their versatility across multiple dimensions. Their platforms deliver robust capabilities across the SDLC to support diverse use cases. Leaders can meet the needs of multiple personas across different teams, such as development, operations and site reliability engineering.

Most Leaders have a strong market penetration across geographies, verticals and organizations of all sizes, and possess a vibrant developer community and a thriving partner ecosystem.

Leaders are well-positioned to remain dominant as the DevSecOps platform market evolves. However, in this rapidly changing market, vendors that lose focus could fall out of the Leaders quadrant.

Challengers

Challengers offer competitive DevSecOps platforms that deliver value for certain industries or use cases. These vendors have shown strong execution in their respective focus areas and are expanding their customer base.

Although Challengers demonstrate the financial strength and commitment to compete in the DevSecOps platform market, they have not demonstrated the vision required to expand their offering beyond their core customer base to serve different types of buyers and address different needs.

To become Leaders, Challengers must improve in their specific areas of caution and match Leaders' ability to establish a compelling product roadmap and a clear vision for the future.

Visionaries

Visionaries focus on innovating their platform technologies and go-to-market strategies based on emerging technology and business trends. They offer a clear product roadmap that demonstrates a strong understanding of market demands.

Despite having a clear vision, Visionaries currently lack visibility outside of their existing customer base or domain. Further, they may lack the resources or expertise to build awareness of their offerings beyond their respective focus area.

To become Leaders, Visionaries must build stronger recognition of their platforms in new market segments and improve their sales and marketing execution.

Niche Players

Niche Players typically specialize in one segment of the DevSecOps platform market or have a relatively limited geographic footprint. They may be startups or small companies just starting to succeed, or vendors focused on a specific subset of use cases, such as container-native or mobile applications. In some cases, Niche Players may not consider DevSecOps platforms strategically significant in their broader portfolio of product offerings.

While Niche Players have not demonstrated the strongest Completeness of Vision or Ability to Execute relative to other vendors in this Magic Quadrant, qualifying for inclusion is quite an accomplishment in this highly competitive global market.

Niche Players may be suitable for organizations that require local presence and support, or need a platform that addresses specific industry use cases and functional requirements. These benefits can offset the viability risks often associated with smaller vendors.

Context

DevSecOps platforms provide software engineering teams with a consolidated set of integrated capabilities that span the entire SDLC. Compared with traditional DevSecOps toolchains, DevSecOps platforms deliver enhanced benefits, including:

- **Improved software security:** DevSecOps platforms integrate and automate security, compliance and governance as part of the development and delivery process. A few DevSecOps platform providers natively support application security capabilities in their offerings (see [Market Guide for Software Supply Chain Security](#)).
- **Better developer experience:** DevSecOps platforms minimize context switching across multiple tools by providing a cohesive, integrated set of capabilities (see [Improve Tooling and Automation for a Great Developer Experience](#)).
- **Modernized application architectures:** DevSecOps platforms provide a strong foundation that enables software engineering teams to take advantage of cloud-native architectures (see [Strategic Roadmap for Adopting Modern Application Architectures and Technologies](#)).
- **Greater visibility into the flow of work:** DevSecOps platforms provide a clear view into software delivery pipelines — from ideation to production — especially when used in conjunction with value stream management. This visibility reduces friction and manual handoffs (see [A Value Stream Approach to Fixing Your Stalled DevOps Initiative](#)).

Market Overview

A growing number of software engineering leaders are modernizing their DevSecOps toolchains by adopting DevSecOps platforms. Gartner estimates that the broad opportunity spanning the application development and IT operations software markets

reached \$25.6 billion in 2024, with DevSecOps platforms representing a significant share of that market. ^{1,2}

A DevSecOps platform can replace many specialized tools across the software delivery life cycle by offering a set of managed, integrated capabilities with built-in support for orchestration. By using DevSecOps platforms, software engineers will not need to dedicate as much time and effort to integrating, managing and orchestrating tools. As a result, software engineering leaders can improve the developer experience and enable their teams to deliver software faster.

Several trends are driving the adoption of DevSecOps platforms, including:

- **Extreme demand for AI-enabled applications:** Software engineering teams must deliver new types of software incorporating AI capabilities. DevSecOps platforms will become even more in demand as organizations adopt MLOps practices to deliver AI-enabled applications.

Related research: [Increase AI Value and Mitigate Risk With Gartner's MLOps Framework](#)

- **A continued focus on AI to drive developer productivity:** The scarcity and cost of developer talent are driving software engineering leaders to use AI to help maximize the productivity of their teams. As AI coding agents become mainstream, code is being produced faster than it can be reviewed and deployed. DevSecOps vendors are pressured to keep pace by enhancing their platforms with AI.

Related research: [Journey Guide to Applying AI to DevSecOps](#)

- **The rise of platform engineering:** Platform engineering teams use DevSecOps platforms to build internal developer platforms and orchestrate platform capabilities as a service to other software engineering teams, which enables product teams to focus on creating customer value.

Related research: [Start and Scale Platform Engineering for Measurable Impact](#)

- **The growing amount of technical debt in DevSecOps toolchains:** A fragmented toolchain results in redundant tools, inefficient spending and a cumbersome experience for developers. Organizations are working to minimize this toolchain-related technical debt to improve the developer experience.

Related research: [Optimize Your DevSecOps Toolchain Selection Strategy](#)

DevSecOps platform vendors are responding to these trends by continuously innovating and expanding platform capabilities, making the market more competitive and difficult to navigate. Software engineering leaders should use our analysis of DevSecOps platform vendors to make a buying decision or to build the business case for modernizing their current toolchain.

⊕ Evidence

⊕ Evaluation Criteria Definitions

Unlock more AI value

With unmatched, proprietary AI insights from Gartner

[Explore the AI Hub ↗](#)

© 2026 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by [Gartner's Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "[Guiding Principles on Independence and Objectivity](#)." Gartner research may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.

